



# CVE-2022-33065

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-33065
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-07-18 14:15:00 UTC
<b>Updated</b>	2023-08-02 17:19:00 UTC
<b>Description</b>	Multiple signed integers overflow in function au_read_header in src/au.c and in functions mat4_open and mat4_read_header

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libsndfile Project	Libsndfile	-	All	All	All

## References

Reference	Source	Link	Tags
Signed integer overflow in src/mat4.c:323 · Issue #789 · libsndfile/libsndfile · GitHub	MISC	<a href="#">github.com</a>	
UndefinedBehaviorSanitizer: multiple signed integer overflow · Issue #833 · libsndfile/libsndfile · GitHub	MISC	<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

199890 Ubuntu Security Notification for libsndfile Vulnerability (USN-6471-1)
673330 EulerOS Security Update for libsndfile (EulerOS-SA-2024-1063)
673469 EulerOS Security Update for libsndfile (EulerOS-SA-2023-3338)
673874 EulerOS Security Update for libsndfile (EulerOS-SA-2023-3306)

[674102](#) EulerOS Security Update for libsndfile (EulerOS-SA-2024-1087)

[691352](#) Free Berkeley Software Distribution (FreeBSD) Security Update for libsndfile\_project (4ade0c4d-7e83-11ee-9a8c-00155d01f201)

[755149](#) SUSE Enterprise Linux Security Update for libsndfile (SUSE-SU-2023:4331-1)

[755150](#) SUSE Enterprise Linux Security Update for libsndfile (SUSE-SU-2023:4330-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)